STATE OF ALABAMA

Information Technology Standard

Standard 640-02S2_Rev A: Virtual Private Networks

1. INTRODUCTION:

A Virtual Private Network (VPN) is a private data network that makes use of the public telecommunication infrastructure, maintaining privacy through the use of a tunneling protocol and security procedures. VPN is the preferred method for users to remotely access (from homes, hotels, off-site offices, etc.) State of Alabama information system resources.

2. OBJECTIVE:

Define requirements for secure remote access VPN connections into the State network.

3. SCOPE:

These requirements apply to all State of Alabama employees, contractors, vendors, and business partners authorized VPN access to the State network (Users), to all personnel responsible for the administration of VPN services and devices (Administrators), and to all Managers responsible for authorizing VPN usage.

4. REQUIREMENTS:

Based on the recommendations of the National Institute of Standards and Technology (NIST) as set forth in Special Publication (SP) 800-77: Guide to IPsec VPNs, and SP 800-113: Guide to SSL VPNs, State of Alabama organizations that deploy and/or manage virtual private networks shall comply with the following requirements:

4.1 VPN MANAGEMENT

Requests for VPN connectivity require the written approval of the agency IT Manager.

VPN connections with business partners and other non-State entities require a written interconnection agreement defining the rules of behavior and security controls that must be maintained and the terms and conditions for sharing data and information resources.

Create and document an access control policy listing the resources that will be accessed through the VPN, the groups or users, the conditions under which the resources should be accessible by the groups, and how the VPN should be used to access the resources. Limit access to specific and necessary information resources.

VPN connections shall allow for monitoring.

To assist in troubleshooting and maintenance, VPN configuration information and technical controls shall be documented.

VPN access accounts shall be reviewed at least quarterly. Inactive accounts shall be disabled in accordance with access management requirements (State IT Standard 620-01S1).

VPN access may be terminated at any time for reasons including, but not limited to, termination of service provider agreements, changes in or termination of employment, request by the system/data owner, non-compliance with security policies, or negative impact on overall network performance attributable to VPN communications.

4.2 VPN ADMINISTRATION

4.2.1 Authentication

Enforce user authentication at the access point before granting VPN access to State network resources. VPN access and authentication shall comply with applicable network access policies and procedures (including password standards, log-in attempts, lock-out policy, etc).

Users will authenticate using their domain login when a trust relationship is established between the RADIUS server and the user's Domain Controller.

When a trust relationship cannot be established, create locally administered user accounts on either the RADIUS server or the VPN Concentrator.

4.2.2 Secure Host

Systems and networks at the VPN endpoints must meet all the security policies and standards applicable to other State systems and networks.

All hosts, including publicly and privately owned personal computers and other remote access devices, connected to State networks via VPN must have up-to-date and properly configured anti-virus software and current operating system service pack and patch level. Hosts may be scanned to ensure compliance with State standards, and users may be denied VPN access if their host system presents an unacceptable risk to State networks.

4.2.3 Technical Controls

VPN communications shall utilize encryption consistent with State encryption standards.

Terminate the VPN on or outside the firewall such that VPN traffic is visible to network intrusion detection/prevention systems.

Split tunneling is not permitted. All traffic to and from the VPN client shall be routed through the VPN tunnel; all other traffic shall be dropped.

Users connected via VPN shall not be allowed simultaneous access to the Internet.

Inactive VPN sessions shall be terminated as specified in State IT Standard 640-02S1: Remote Access Controls.

Log VPN activity and establish effective log review procedures. Auditors should be able to extract detailed usage information from VPN logs. At a minimum, VPN devices shall log all successful and failed login attempts.

Monitor VPN usage and test VPN security controls on a regular basis (at least quarterly) for security and performance.

Any unusual VPN event that may indicate unauthorized use of VPN services shall immediately be reported as a cyber security incident following applicable reporting procedures.

5. DEFINITIONS:

IPSEC: Internet Protocol Security (IPsec) is a framework for a set of protocols for security at the network or packet processing layer of network communication designed to provide private communications over public networks.

RADIUS: Remote Authentication Dial-In User Service, RADIUS, is an authentication, authorization, and accounting (AAA) protocol for network access application.

SPLIT TUNNELING: Term used to describe a multiple-branch networking path. In a VPN context, a secure tunnel is established to the VPN concentrator and other traffic is sent directly to different remote locations without passing through the VPN concentrator. This can expose the State's networked resources to attack and can make State resources accessible to anyone from non-trusted networks.

SSL VPN: Secure Sockets Layer (SSL) Virtual Private Network (VPN) is a form of VPN that can be used with a standard Web browser. In contrast to the IPsec VPN, an SSL VPN does not require the installation of specialized client software on the end user's computer.

6. ADDITIONAL INFORMATION:

6.1 POLICY

Information Technology Policy 640-02: Remote Access

6.2 RELATED DOCUMENTS

Information Technology Standard 620-01S1: Access Management

Information Technology Standard 640-01S1: Interconnecting IT Systems

Information Technology Standard 640-01S2: Secure Web Application Deployment

Information Technology Standard 640-02S1: Remote Access Controls

Information Technology Standard 670-06S1: Log Management

Information Technology Standard 680-03S1: Encryption

Signed by Art Bess, Assistant Director

7. DOCUMENT HISTORY:

Version	Release Date	Comments
Original	2/16/2007	
Rev A	2/13/2009	Added requirements for access control policy, documentation, session time-out, logging, and quarterly testing of security controls.